Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/016450

International filing date: 07 September 2005 (07.09.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-298245
Filing date: 12 October 2004 (12.10.2004)

Date of receipt at the International Bureau: 13 October 2005 (13.10.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

BEST AVAILABLE COPY

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００４年１０月１２日
出願番号 Application Number:	特願２００４－２９８２４５
パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号 The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is	ＪＰ２００４－２９８２４５
出願人 Applicant(s):	日本電信電話株式会社

２００５年　９月２８日

特許庁長官
Commissioner,
Japan Patent Office

中嶋　誠

【書類名】　特許願
【整理番号】　NTTH166072
【提出日】　平成16年10月12日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/56
　　H04L 12/46
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　三好　潤
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　長島　雅夫
【特許出願人】
　【識別番号】　000004226
　【氏名又は名称】　日本電信電話株式会社
【代理人】
　【識別番号】　100089118
　【弁理士】
　【氏名又は名称】　酒井　宏明
【選任した代理人】
　【識別番号】　100114306
　【弁理士】
　【氏名又は名称】　中辻　史郎
【手数料の表示】
　【予納台帳番号】　036711
　【納付金額】　16,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0310351

【書類名】特許請求の範囲
【請求項１】
ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御システムであって、
前記中継装置は、
前記ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を記憶する正規アドレス情報記憶手段と、
前記ゲート装置により前記通信機器への攻撃が検知された場合に、前記正規アドレス情報記憶手段に記憶した正規アドレス情報を当該ゲート装置に転送する転送手段とを備え、
前記ゲート装置は、
前記ネットワークから受信されたパケットによる攻撃を検知する攻撃検知手段と、
前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなう通過制御手段とを備えたことを特徴とするサービス不能攻撃防御システム。
【請求項２】
前記ゲート装置は、前記攻撃検知手段により攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成手段と、前記容疑シグネチャ生成手段により生成された容疑シグネチャを前記中継装置に送信し、その結果返信された正規アドレス情報を取得する正規アドレス情報取得手段とをさらに備え、前記転送手段は、前記ゲート装置から前記容疑シグネチャを受信した際に、前記正規アドレス情報記憶手段に記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送することを特徴とする請求項１に記載のサービス不能攻撃防御システム。
【請求項３】
前記通過制御手段は、前記正規アドレス情報取得手段により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手段と、前記ネットワークから受信したパケットのうち前記正規条件情報生成手段により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限手段とを備えたことを特徴とする請求項２に記載のサービス不能攻撃防御システム。
【請求項４】
前記ゲート装置は、前記容疑シグネチャ生成手段により生成された容疑シグネチャに該当するパケットのうち、前記正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成手段をさらに備え、前記パケット制限手段は、前記容疑シグネチャ生成手段により生成された容疑シグネチャおよび前記正規シグネチャ生成手段により生成された正規シグネチャに基づいて前記ネットワークから受信したパケットの通過を制限することを特徴とする請求項３に記載のサービス不能攻撃防御システム。
【請求項５】
前記ゲート装置は、前記正規シグネチャ生成手段により生成された正規シグネチャを前記中継装置に転送するシグネチャ転送手段をさらに備えたことを特徴とする請求項４に記載のサービス不能攻撃防御システム。
【請求項６】
ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御方法であって、
前記中継装置が前記ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を正規アドレス情報記憶部に格納する正規アドレス情報格納工程と、
前記ゲート装置により前記通信機器への攻撃が検知された場合に、前記正規アドレス情

報記憶部に記憶した正規アドレス情報を当該ゲート装置に転送する転送工程と、
前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなう通過制御工程と
を含んだことを特徴とするサービス不能攻撃防御方法。
【請求項７】
前記ゲート装置が前記攻撃検知工程により攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成工程と、前記容疑シグネチャ生成工程により生成された容疑シグネチャを前記中継装置に送信し、その結果返信された正規アドレス情報を取得する正規アドレス情報取得工程とをさらに含み、前記転送工程は、前記ゲート装置から前記容疑シグネチャを受信した際に、前記正規アドレス情報記憶部に記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送することを特徴とする請求項６に記載のサービス不能攻撃防御方法。
【請求項８】
前記通過制御工程は、前記正規アドレス情報取得工程により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成工程と、前記ネットワークから受信したパケットのうち前記正規条件情報生成工程により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限工程とを含んだことを特徴とする請求項７に記載のサービス不能攻撃防御方法。
【請求項９】
前記ゲート装置が前記容疑シグネチャ生成工程により生成された容疑シグネチャに該当するパケットのうち、前記正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成工程をさらに含み、前記パケット制限工程は、前記容疑シグネチャ生成工程により生成された容疑シグネチャおよび前記正規シグネチャ生成工程により生成された正規シグネチャに基づいて前記ネットワークから受信したパケットの通過を制限することを特徴とする請求項８に記載のサービス不能攻撃防御方法。
【請求項１０】
ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御プログラムであって、
前記中継装置が前記ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を正規アドレス情報記憶部に格納する正規アドレス情報格納手順と、
前記ゲート装置により前記通信機器への攻撃が検知された場合に、前記正規アドレス情報記憶部に記憶した正規アドレス情報を当該ゲート装置に転送する転送手順と、
前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなう通過制御手順と
を含んだことを特徴とするサービス不能攻撃防御プログラム。
【請求項１１】
前記ゲート装置が前記攻撃検知手順により攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成手順と、前記容疑シグネチャ生成手順により生成された容疑シグネチャを前記中継装置に送信し、その結果返信された正規アドレス情報を取得する正規アドレス情報取得手順とをさらに含み、前記転送手順は、前記ゲート装置から前記容疑シグネチャを受信した際に、前記正規アドレス情報記憶部に記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送することを特徴とする請求項１０に記載のサービス不能攻撃防御プログラム。
【請求項１２】
前記通過制御手順は、前記正規アドレス情報取得手順により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手順

と、前記ネットワークから受信したパケットのうち前記正規条件情報生成手順により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限手順とを含んだことを特徴とする請求項１１に記載のサービス不能攻撃防御プログラム。

【請求項１３】

前記ゲート装置が前記容疑シグネチャ生成手順により生成された容疑シグネチャに該当するパケットのうち、前記正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成手順をさらに含み、前記パケット制限手順は、前記容疑シグネチャ生成手順により生成された容疑シグネチャおよび前記正規シグネチャ生成手順により生成された正規シグネチャに基づいて前記ネットワークから受信したパケットの通過を制限することを特徴とする請求項１２に記載のサービス不能攻撃防御プログラム。

【書類名】明細書
【発明の名称】サービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラム
【技術分野】
【０００１】
この発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくはこの中継装置で通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラムに関し、特に、防御対象の通信機器に対して攻撃をおこなわない非攻撃パケットの条件を表す正規条件情報を容易に管理することができるサービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラムに関する。
【背景技術】
【０００２】
従来、ネットワークを介した攻撃としてサービス不能攻撃および分散型サービス不能攻撃（Distributed Denial of Service Attack、以下単に「ＤＤｏｓ攻撃」と言う）が知られている。かかるＤＤｏｓ攻撃から通信機器を防御する分散型サービス不能攻撃防御システムでは、攻撃対象となる通信機器とネットワークとの間に設けられたゲートウェイ装置やネットワークを構成するルータ装置がパケットを制限することになる。具体的には、ネットワークを介して通信機器に向けて送信されたパケットを正規パケット、容疑パケットまたは不正パケットに分類し、通信機器に送信されるパケットを制限していた（例えば、特許文献１参照）。
【０００３】
このような従来の分散型サービス不能攻撃防御システムにおいては、あらかじめ登録された攻撃検知条件に基づいてゲートウェイ装置が攻撃を検知すると、攻撃検知されたパケットの特徴を示す容疑シグネチャが生成され、生成された容疑シグネチャがネットワークを構成するルータ装置等の中継装置に転送される。
【０００４】
一方、容疑シグネチャに当てはまるパケットのうち通信機器に対する攻撃とみなされないパケット（以下「非攻撃パケット」と言う）の特徴を表す正規シグネチャが、あらかじめ登録された正規条件情報に基づいてゲートウェイ装置によって生成され、生成された正規シグネチャがネットワークを構成するルータ装置等の中継装置に転送される。
【０００５】
容疑シグネチャおよび正規シグネチャが転送された中継装置並びにゲートウェイ装置によって中継されるパケットは、容疑シグネチャおよび正規シグネチャに基づいてシェーピングやフィルタリング等の処理が施される。
【０００６】
このように、従来の分散型サービス不能攻撃防御システムは、攻撃を行うパケットの通過を出来るだけ攻撃元の近くで制限することによって、攻撃を行うパケット（以下「攻撃パケット」と言う）による悪影響を出来るだけ小さくするようになっている。
【０００７】
【特許文献１】特開２００３－２８３５５４号公報
【発明の開示】
【発明が解決しようとする課題】
【０００８】
しかしながら、従来の分散型サービス不能攻撃防御システムにおいては、攻撃から防御する対象の通信機器に対する非攻撃パケットの条件を表す正規条件情報の追加や変更等の管理がゲートウェイ装置のオペレータによって行われるため、正規条件情報の管理が煩雑になるといった課題があった。
【０００９】

本発明は、上述した従来技術による問題点を解消するためになされたものであり、防御対象の通信機器に対して攻撃をおこなわない非攻撃パケットの条件を表す正規条件情報を容易に管理することができるサービス不能攻撃防御方法、サービス不能攻撃防御装置およびサービス不能攻撃防御プログラムを提供することを目的とする。

【課題を解決するための手段】

【００１０】

上述した課題を解決し、目的を達成するため、本発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御システムであって、前記中継装置は、前記ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を記憶する正規アドレス情報記憶手段と、前記ゲート装置により前記通信機器への攻撃が検知された場合に、前記正規アドレス情報記憶手段に記憶した正規アドレス情報を当該ゲート装置に転送する転送手段とを備え、前記ゲート装置は、前記ネットワークから受信されたパケットによる攻撃を検知する攻撃検知手段と、前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなう通過制御手段とを備えたことを特徴とする。

【００１１】

この発明によれば、中継装置がネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を記憶しておき、ゲート装置により通信機器への攻撃が検知された場合に、記憶した正規アドレス情報を当該ゲート装置に転送し、ゲート装置は、中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなうこととしたので、各中継装置が保持する正規アドレス情報が攻撃を検出したゲート装置に自動的に送信することができ、ネットワークを介した攻撃を行わない非攻撃パケットの送信元が追加または変更された場合に、正規条件情報を必要なゲート装置にのみ無駄なく登録することができ、またゲート装置がネットワークに追加された場合に、追加されたゲート装置に対して必要な分だけの正規条件情報を無駄なく登録することができる。

【００１２】

また、本発明は、上記発明において、前記ゲート装置は、前記攻撃検知手段により攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成手段と、前記容疑シグネチャ生成手段により生成された容疑シグネチャを前記中継装置に送信し、その結果返信された正規アドレス情報を取得する正規アドレス情報取得手段とをさらに備え、前記転送手段は、前記ゲート装置から前記容疑シグネチャを受信した際に、前記正規アドレス情報記憶手段に記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送することを特徴とする。

【００１３】

この発明によれば、ゲート装置は、攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成して中継装置に送信し、中継装置では、ゲート装置から容疑シグネチャを受信した際に、記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送し、ゲート装置はその結果返信された正規アドレス情報を取得することとしたので、容疑シグネチャの送信を契機として必要なゲート装置が効率良く正規アドレス情報を取得することができる。

【００１４】

また、本発明は、上記発明において、前記通過制御手段は、前記正規アドレス情報取得手段により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手段と、前記ネットワークから受信したパケットのうち前記正規条件情報生成手段により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限手段とを備えたことを特徴とする。

【００１５】
この発明によれば、取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限することとしたので、正規アドレス情報から生成した正規条件情報に基づいて適正なパケットの通過制御をおこなうことができる。
【００１６】
また、本発明は、上記発明において、前記ゲート装置は、前記容疑シグネチャ生成手段により生成された容疑シグネチャに該当するパケットのうち、前記正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成手段をさらに備え、前記パケット制限手段は、前記容疑シグネチャ生成手段により生成された容疑シグネチャおよび前記正規シグネチャ生成手段により生成された正規シグネチャに基づいて前記ネットワークから受信したパケットの通過を制限することを特徴とする。
【００１７】
この発明によれば、ゲート装置が容疑シグネチャに該当するパケットのうち、正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成し、生成された容疑シグネチャおよび正規シグネチャに基づいてネットワークから受信したパケットの通過を制限することとしたので、容疑シグネチャおよび正規シグネチャという指標を用いて効率良くパケットの通過制御をおこなうことができる。
【００１８】
また、本発明は、上記発明において、前記ゲート装置は、前記正規シグネチャ生成手段により生成された正規シグネチャを前記中継装置に転送するシグネチャ転送手段をさらに備えたことを特徴とする。
【００１９】
この発明によれば、ゲート装置が生成された正規シグネチャを中継装置に転送することとしたので、ゲート装置のみならず中継装置においても効率良くパケットの通過制御をおこなうことができる。
【００２０】
また、本発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御方法であって、前記中継装置が前記ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を正規アドレス情報記憶部に格納する正規アドレス情報格納工程と、前記ゲート装置により前記通信機器への攻撃が検知された場合に、前記正規アドレス情報記憶部に記憶した正規アドレス情報を当該ゲート装置に転送する転送工程と、前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなう通過制御工程とを含んだことを特徴とする。
【００２１】
この発明によれば、中継装置がネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を記憶しておき、ゲート装置により通信機器への攻撃が検知された場合に、記憶した正規アドレス情報を当該ゲート装置に転送し、ゲート装置は、中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなうこととしたので、各中継装置が保持する正規アドレス情報が攻撃を検出したゲート装置に自動的に送信することができ、ネットワークを介した攻撃を行わない非攻撃パケットの送信元が追加または変更された場合に、正規条件情報を必要なゲート装置にのみ無駄なく登録することができ、またゲート装置がネットワークに追加された場合に、追加されたゲート装置に対して必要な分だけの正規条件情報を無駄なく登録することができる。
【００２２】
また、本発明は、上記発明において、前記ゲート装置が前記攻撃検知工程により攻撃が

検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成工程と、前記容疑シグネチャ生成工程により生成された容疑シグネチャを前記中継装置に送信し、その結果返信された正規アドレス情報を取得する正規アドレス情報取得工程とをさらに含み、前記転送工程は、前記ゲート装置から前記容疑シグネチャを受信した際に、前記正規アドレス情報記憶部に記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送することを特徴とする。

【００２３】

この発明によれば、ゲート装置は、攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成して中継装置に送信し、中継装置では、ゲート装置から容疑シグネチャを受信した際に、記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送し、ゲート装置はその結果返信された正規アドレス情報を取得することとしたので、容疑シグネチャの送信を契機として必要なゲート装置が効率良く正規アドレス情報を取得することができる。

【００２４】

また、本発明は、上記発明において、前記通過制御工程は、前記正規アドレス情報取得工程により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成工程と、前記ネットワークから受信したパケットのうち前記正規条件情報生成工程により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限工程とを含んだことを特徴とする。

【００２５】

この発明によれば、取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限することとしたので、正規アドレス情報から生成した正規条件情報に基づいて適正なパケットの通過制御をおこなうことができる。

【００２６】

また、本発明は、上記発明において、前記ゲート装置が前記容疑シグネチャ生成工程により生成された容疑シグネチャに該当するパケットのうち、前記正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成工程をさらに含み、前記パケット制限工程は、前記容疑シグネチャ生成工程により生成された容疑シグネチャおよび前記正規シグネチャ生成工程により生成された正規シグネチャに基づいて前記ネットワークから受信したパケットの通過を制限することを特徴とする。

【００２７】

この発明によれば、ゲート装置が容疑シグネチャに該当するパケットのうち、正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成し、生成された容疑シグネチャおよび正規シグネチャに基づいてネットワークから受信したパケットの通過を制限することとしたので、容疑シグネチャおよび正規シグネチャという指標を用いて効率良くパケットの通過制御をおこなうことができる。

【００２８】

また、本発明は、ネットワークの一部を形成する中継装置とサービス不能攻撃対象となる通信機器との間に介在するゲート装置若しくは前記中継装置で前記通信機器に対するサービス不能攻撃を防御するサービス不能攻撃防御プログラムであって、前記中継装置が前記ネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を正規アドレス情報記憶部に格納する正規アドレス情報格納手順と、前記ゲート装置により前記通信機器への攻撃が検知された場合に、前記正規アドレス情報記憶部に記憶した正規アドレス情報を当該ゲート装置に転送する転送手順と、前記中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなう通過制御手順とを含んだことを特徴とする。

【００２９】

この発明によれば、中継装置がネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を記憶しておき、ゲート装置により通信機器への攻撃が検知された場合に、記憶した正規アドレス情報を当該ゲート装置に転送し、ゲート装置は、中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなうこととしたので、各中継装置が保持する正規アドレス情報が攻撃を検出したゲート装置に自動的に送信することができ、ネットワークを介した攻撃を行わない非攻撃パケットの送信元が追加または変更された場合に、正規条件情報を必要なゲート装置にのみ無駄なく登録することができ、またゲート装置がネットワークに追加された場合に、追加されたゲート装置に対して必要な分だけの正規条件情報を無駄なく登録することができる。

【００３０】

また、本発明は、上記発明において、前記ゲート装置が前記攻撃検知手順により攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成手順と、前記容疑シグネチャ生成手順により生成された容疑シグネチャを前記中継装置に送信し、その結果返信された正規アドレス情報を取得する正規アドレス情報取得手順とをさらに含み、前記転送手順は、前記ゲート装置から前記容疑シグネチャを受信した際に、前記正規アドレス情報記憶部に記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送することを特徴とする。

【００３１】

この発明によれば、ゲート装置は、攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成して中継装置に送信し、中継装置では、ゲート装置から容疑シグネチャを受信した際に、記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送し、ゲート装置はその結果返信された正規アドレス情報を取得することとしたので、容疑シグネチャの送信を契機として必要なゲート装置が効率良く正規アドレス情報を取得することができる。

【００３２】

また、本発明は、上記発明において、前記通過制御手順は、前記正規アドレス情報取得手順により取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成する正規条件情報生成手順と、前記ネットワークから受信したパケットのうち前記正規条件情報生成手順により生成された正規条件情報に示された条件に適合するパケットの通過を許容しつつ、前記通信機器へ攻撃をおこなうパケットの通過を制限するパケット制限手順とを含んだことを特徴とする。

【００３３】

この発明によれば、取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限することとしたので、正規アドレス情報から生成した正規条件情報に基づいて適正なパケットの通過制御をおこなうことができる。

【００３４】

また、本発明は、上記発明において、前記ゲート装置が前記容疑シグネチャ生成手順により生成された容疑シグネチャに該当するパケットのうち、前記正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成手順をさらに含み、前記パケット制限手順は、前記容疑シグネチャ生成手順により生成された容疑シグネチャおよび前記正規シグネチャ生成手順により生成された正規シグネチャに基づいて前記ネットワークから受信したパケットの通過を制限することを特徴とする。

【００３５】

この発明によれば、ゲート装置が容疑シグネチャに該当するパケットのうち、正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成し、生成された容疑シグネチャおよび正規シグネチャに基づいてネットワークから受信したパケットの通過を制限することとしたので、容疑シグネチャおよび正規シグネチャという指標を用い

て効率良くパケットの通過制御をおこなうことができる。

【発明の効果】

【００３６】

本発明によれば、中継装置がネットワーク上に所在する正当な装置から受信した非攻撃パケットの送信元を示す正規アドレス情報を記憶しておき、ゲート装置により通信機器への攻撃が検知された場合に、記憶した正規アドレス情報を当該ゲート装置に転送し、ゲート装置は、中継装置から受け取った正規アドレス情報から生成された非攻撃パケットの条件を示す正規条件情報に基づいてパケットの通過制御をおこなうよう構成したので、各中継装置が保持する正規アドレス情報が攻撃を検出したゲート装置に自動的に送信することができ、ネットワークを介した攻撃を行わない非攻撃パケットの送信元が追加または変更された場合に、正規条件情報を必要なゲート装置にのみ無駄なく登録することができ、またゲート装置がネットワークに追加された場合に、追加されたゲート装置に対して必要な分だけの正規条件情報を無駄なく登録することができる。

【００３７】

また、本発明によれば、ゲート装置は、攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成して中継装置に送信し、中継装置では、ゲート装置から容疑シグネチャを受信した際に、記憶した正規アドレス情報を当該容疑シグネチャの送信元のゲート装置に転送し、ゲート装置はその結果返信された正規アドレス情報を取得するよう構成したので、容疑シグネチャの送信を契機として必要なゲート装置が効率良く正規アドレス情報を取得することができる。

【００３８】

また、本発明によれば、取得された正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限するよう構成したので、正規アドレス情報から生成した正規条件情報に基づいて適正なパケットの通過制御をおこなうことができる。

【００３９】

また、本発明によれば、ゲート装置が容疑シグネチャに該当するパケットのうち、正規条件情報に示された条件に適合するパケットの特徴を表す正規シグネチャを生成し、生成された容疑シグネチャおよび正規シグネチャに基づいてネットワークから受信したパケットの通過を制限するよう構成したので、容疑シグネチャおよび正規シグネチャという指標を用いて効率良くパケットの通過制御をおこなうことができる。

【００４０】

また、本発明によれば、ゲート装置が生成された正規シグネチャを中継装置に転送するよう構成したので、ゲート装置のみならず中継装置においても効率良くパケットの通過制御をおこなうことができる。

【発明を実施するための最良の形態】

【００４１】

以下に添付図面を参照して、この発明に係るサービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラムの好適な実施の形態を詳細に説明する。

【実施例】

【００４２】

図１は、本実施例に係る分散型サービス不能攻撃防御システム１の構成を示すブロック図である。同図に示す分散型サービス不能攻撃防御システム１は、通信機器７への分散型サービス不能攻撃を主としてゲート装置８で防御するシステムである。具体的には、ネットワーク２上に所在する正当な装置（アドレス発行サーバ１０）により送信された非攻撃パケットの送信元を示す正規アドレス情報をゲート装置８が取得し、取得した正規アドレス情報に基づいてゲート装置８が非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち正規条件情報に示された条件に適合するパケット

の通過を許容しつつ、通信機器７へ攻撃をおこなうパケットの通過を制限するようにしている。なお、このゲート装置８が正規条件情報に基づいて生成した正規シグネチャ並びに容疑シグネチャは中継装置６などに転送され、中継装置でのフィルタリングを可能ならしめている。

【００４３】

従来、かかる正規アドレス情報の追加や変更等の管理は、ゲート装置８のオペレータによって行われていたため、正規条件情報の管理が煩雑になるという問題があった。このため、本実施例では、かかる正規アドレス情報の追加をゲート装置８のオペレータに担わせるのではなく、アドレス発行サーバ１０などの正当な端末から正規アドレス情報を取得することとしている。このため、本実施例によれば、ゲート装置８のオペレータの管理負担を軽減することができる。

【００４４】

ここで、このゲート装置８が正規アドレス情報を取得する際に、本実施例では、アドレス発行サーバ１０が中継装置６に対して正規アドレス情報を送信し（図１のステップ１）、この中継装置６に正規アドレス情報を記憶させ（図１のステップ２）、ゲート装置８が攻撃を検知したパケットの特徴を表す容疑シグネチャを生成して生成した容疑シグネチャを中継装置６に送信すると（図１のステップ３）、あらかじめ記憶した正規アドレス情報をゲート装置８に転送し（図１のステップ４）、ゲート装置８が正規アドレス情報に基づいて正規条件情報を自動生成する（図１のステップ５）こととしている。

【００４５】

次に、この分散型サービス不能攻撃防御システム１のシステム構成について説明する。図１に示すように、この分散型サービス不能攻撃防御システム１は、ネットワーク２を介して伝送されるパケットを中継する複数の中継装置３～６と、ネットワーク２を介して通信機器７に送信されるパケットの通過を制限するゲート装置８とを備えている。なお、図１に示した分散型サービス不能攻撃防御システム１の構成は一例を示すものであり、中継装置およびゲート装置等の数量やネットワーク構成を限定するものではない。

【００４６】

ゲート装置８は、ネットワーク間接続機器であるゲートウェイ装置などによって構成され、コンピュータ装置等によって構成される通信機器７を含む構内情報通信網（Local Area Network、以下単に「ＬＡＮ」と記載する。）１４に接続されている。また、中継装置３～６は、ルータ装置によってそれぞれ構成されている。なお、この中継装置３～６は、ブリッジによって構成することもできる。

【００４７】

ここで、中継装置３は、中継装置４およびゲート装置８に接続され、中継装置４は、通信機器１５および中継装置３に接続され、中継装置５は、通信機器１６および中継装置６に接続され、中継装置６は、中継装置５、エッジルータ１１およびゲート装置８に接続されている。

【００４８】

図２は、図１に示したゲート装置８の構成を示すブロック図である。図２に示すように、このゲート装置８は、ネットワーク２から受信されたパケットによる攻撃を検知する攻撃検知部２０と、攻撃が検知されたパケットの特徴を表す容疑シグネチャを生成する容疑シグネチャ生成部２１と、通信機器７に対する攻撃とみなされないパケット（非攻撃パケット）の条件を表す正規条件情報を格納する正規条件情報格納部２２と、正規条件情報格納部２２に格納される正規条件情報を生成する正規条件情報生成部２３と、容疑シグネチャに当てはまるパケットのうち、正規条件情報に表された条件に合うパケットの特徴を表す正規シグネチャを生成する正規シグネチャ生成部２４と、容疑シグネチャに当てはまるパケットのうち、通信機器７に対する攻撃とみなすパケットの特徴を表す不正シグネチャを生成する不正シグネチャ生成部２５と、容疑シグネチャ、正規シグネチャおよび不正シグネチャに基づいてネットワーク２から受信されたパケットの通過を制限するパケット制限部２６と、容疑シグネチャおよび正規シグネチャを隣接関係にある中継装置３および中

継装置６に転送するシグネチャ転送部２７と、ネットワーク２に接続された各装置と通信を行うネットワークインタフェイス２８とを備えている。

【００４９】

攻撃検知部２０は、あらかじめ設定された攻撃検知条件に基づいて攻撃を検知する処理部である。図３は、攻撃検知条件の一例を示す図である。図３において、攻撃検知条件は、検知属性、検知閾値および検知時間の組からなる３組のレコードで構成される。検知属性は、検知対象とするパケットの属性を示し、検知閾値は、検知対象となるパケットの伝送レートの閾値を示し、検知時間は、検知対象となるパケットの伝送レートが検知閾値を超える時間の閾値を示している。

【００５０】

例えば、１番目の検知条件は、宛先のアドレス情報が192.168.1.1であり（Dst=192.168.1.1/32）、トランスポート層のプロトコルがＴＣＰ（Transmission Control Protocol）であり（Protocol=TCP）、ＴＣＰポート番号が８０である（Port=80）パケットが検知対象となり、この検知対象のパケットの伝送レートが５００kbpsを超えた状態が１０秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。

【００５１】

同様に、２番目の検知条件は、宛先のアドレス情報が192.168.1.2であり（Dst=192.168.1.2/32）、トランスポート層のプロトコルがＵＤＰ（User datagram protocol）である（Protocol=UDP）パケットが検知対象となり、この検知対象のパケットの伝送レートが３００kbpsを超えた状態が１０秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。

【００５２】

また、３番目の検知条件は、宛先のアドレス情報が192.168.1.0～192.168.1.255の範囲内である（Dst=192.168.1.0/24）パケットが検知対象となり、この検知対象のパケットの伝送レートが１Mbpsを超えた状態が２０秒以上続いた場合には、検知対象のパケットによる攻撃として検知される。

【００５３】

このように、検知対象のパケットによる攻撃が攻撃検知部２０によって検知されると、容疑シグネチャ生成部２１は、検知対象のパケットの特徴を表す容疑シグネチャを生成する。例えば、図３における攻撃検知条件の１番目の検知条件に合う攻撃が検知された場合には、容疑シグネチャ生成部２１は、宛先のアドレス情報が192.168.1.1であり、トランスポート層のプロトコルがＴＣＰであり、ＴＣＰポート番号が８０であるパケットを示す容疑シグネチャを生成する。なお、容疑シグネチャは、対象となるパケットに対するシェーピングやフィルタリング等の処理や、この処理に関するパラメータ等を含むようにしてもよい。

【００５４】

正規条件情報格納部２２は、フラッシュメモリなどの不揮発性の記憶媒体によって構成されている。図４は、正規条件情報格納部２２に格納される正規条件情報の一例を示す図である。図４において、正規条件情報は攻撃とみなされない条件である正規条件で構成される。

【００５５】

例えば、１番目の正規条件によって、送信元のアドレス情報が172.16.10.0～172.16.10.255の範囲内である（Src=172.16.10.0/24）パケットは、攻撃とみなされない。同様に、２番目の正規条件によって、サービスタイプ（Type of Service）が０ｘ０１である（TOS=0x01）パケットは、攻撃とみなされない。

【００５６】

正規条件情報生成部２３は、本実施例の最も重要な特徴部分をなす処理部であり、オペレータの処理行為を伴うことなく正規条件情報格納部２２に格納された正規条件情報の自動更新をおこなう。従来、かかる正規条件情報の管理はオペレータに委ねられていたが、本実施例では、かかる正規条件情報を自動更新している。

【００５７】
具体的には、この正規条件情報生成部２３は、ネットワーク２を介した攻撃を行わないパケットの送信元を表す正規アドレス情報が隣接する中継装置３または６から送信され、送信された正規アドレス情報がネットワークインタフェイス２８に受信された場合に、この正規アドレス情報に基づいて正規条件情報を生成し、生成した正規条件情報を以って正規条件情報格納部２２に格納された正規条件情報を更新する。すなわち、正規アドレス情報を送信アドレスとしたパケットは、通信機器７に対する攻撃とみなされないものとなる。なお、ここでは正規条件情報の追加を自動的におこなう点を強調したが、正規条件情報格納部２２に格納された正規条件情報は、ゲート装置８のオペレータによって追加、削除、変更などの編集ができるようにしてもよい。
【００５８】
正規シグネチャ生成部２４は、容疑シグネチャ生成部２１によって生成された容疑シグネチャに当てはまるパケットのうち、正規条件情報に表された条件に合うパケットの特徴を表す正規シグネチャを生成する処理部である。
【００５９】
例えば、この正規シグネチャ生成部２４は、攻撃検知部２０によって図３に示した１番目の攻撃検知条件に合う攻撃が検知された場合には、図４に示した正規条件情報に基づいて、宛先のアドレス情報が192.168.1.1であり、トランスポート層のプロトコルがＴＣＰであり、ＴＣＰポート番号が８０であり、送信元のアドレス情報が172.16.10.0～172.16.10.255の範囲内であるパケットを示す正規シグネチャと、宛先のアドレス情報が192.168.1.1であり、トランスポート層のプロトコルがＴＣＰであり、ＴＣＰポート番号が80であり、サービスタイプが0x01であるパケットを示す正規シグネチャとを生成する。
【００６０】
不正シグネチャ生成部２５は、容疑シグネチャ生成部２１によって生成された容疑シグネチャに当てはまるパケットのうち、不正条件に合うパケットの特徴を表す不正シグネチャを生成する処理部である。
【００６１】
図５は、不正条件の一例を示す図である。図５において、１番目の不正条件は、500kbps以上の伝送レートで３０秒以上連続送信されているパケットを示している。同様に、２番目の不正条件は、300kbps以上の伝送レートで１５秒以上連続送信されているICMP（Internet Control Message Protocol）に準拠したエコー応答（Echo Reply）パケットを示し、３番目の不正条件は、300kbps以上の伝送レートで１５秒以上連続送信されている分割送信されたフラグメントパケットを示している。
【００６２】
パケット制限部２６は、容疑シグネチャ生成部２１によって生成された容疑シグネチャと正規シグネチャ生成部２４によって生成された正規シグネチャと不正シグネチャ生成部２５によって生成された不正シグネチャに基づいてネットワークインタフェイス２８によって受信されたパケットの通過を制限するようになっている。
【００６３】
具体的には、パケット制限部２６は、不正シグネチャに当てはまるパケットを廃棄し、正規シグネチャに当てはまるパケットに対しては制限を加えずに通過させ、容疑シグネチャに当てはまるパケットに対しては容疑シグネチャに示された処理等に基づいて伝送帯域を絞った経路を介して通過させるようになっている。
【００６４】
シグネチャ転送部２７は、容疑シグネチャおよび正規シグネチャを隣接関係にある中継装置３および中継装置６に転送する処理部であり、中継装置３および中継装置６は、さらに隣接関係にある中継装置にパケットを転送する。なお、隣接関係とは、本発明に係るゲート装置および中継装置における隣接関係であり、物理的な接続関係とは異なる。
【００６５】
図６は、図１に示した中継装置６の構成を示す機能ブロック図である。なお、ここでは

説明の便宜上中継装置６の構成を説明するが、他の中継装置３～５についても中継装置６と同様に構成されている。この中継装置６は、入力ポート３０と、パケットをルーティングするためのスイッチ３１と、出力ポート３２と、不正シグネチャを生成する不正シグネチャ生成部３５と、不正シグネチャならびにゲート装置８によって転送された容疑シグネチャおよび正規シグネチャに基づいて入力ポート３０に入力されたパケットの通過を制限するパケット制限部３６と、容疑シグネチャおよび正規シグネチャを隣接関係にある中継装置５に転送するシグネチャ転送部３７と、中継装置６の保持する正規アドレス情報を格納する正規アドレス情報格納部３８と、正規アドレス情報格納部３８に格納された正規アドレス情報を送信する正規アドレス情報送信部３９を備えている。

【００６６】

ここで、不正シグネチャ生成部３５、パケット制限部３６およびシグネチャ転送部３７は、ゲート装置８を構成する不正シグネチャ生成部２５、パケット制限部２６およびシグネチャ転送部２７とそれぞれ同様に構成されるため、詳細な説明は省略する。なお、中継装置６は、ゲート装置８と同様に、攻撃検知部、容疑シグネチャ生成部、正規条件情報格納部および正規シグネチャ生成部を備えるようにしてもよい。

【００６７】

シグネチャ転送部３７は、パケット制限部３６によってパケットの通過が制限された後、制限された伝送レートを超えた容疑シグネチャに当てはまるパケットが入力ポート３０に受信されているか否かを判断し、制限された伝送レートを超えた容疑シグネチャに当てはまるパケットが入力ポート３０に受信されていると判断した場合には、容疑シグネチャおよび正規シグネチャを転送し、制限された伝送レートを超えた容疑シグネチャに当てはまるパケットが入力ポート３０に受信されていると判断しなかった場合には、容疑シグネチャおよび正規シグネチャを転送しない。

【００６８】

また、図１に示した構成においては、中継装置４および中継装置５には、容疑シグネチャおよび正規シグネチャを転送する中継装置が存在しないため、シグネチャ転送部３７による容疑シグネチャおよび正規シグネチャの転送は行われない。

【００６９】

このように、ゲート装置８によって攻撃が検知された場合には、容疑シグネチャおよび正規シグネチャが生成され、生成された容疑シグネチャおよび正規シグネチャが各中継装置３～６に転送され、ゲート装置８および中継装置３～６においてパケットのシェーピングやフィルタリング等の処理が施される。このため、分散型サービス不能攻撃防御システム１においては、例えば、ゲート装置８によって検知された攻撃が通信機器１５を介して行われている場合には、攻撃を行うパケットの通過が攻撃元の近く、すなわち中継装置４で制限され、攻撃を行うパケットによる悪影響が小さくなる。

【００７０】

アドレス情報格納部３８は、不揮発性の記憶媒体によって構成されており、正規アドレス情報を保持する。

【００７１】

図１において、ＬＡＮ９は、エッジルータ１１を介してネットワーク２と接続されるとともに、コンピュータ装置等の通信機器１２、１３が接続されている。ここで、ＬＡＮ９では、ネットワーク２を介した攻撃を行わないものとする。

【００７２】

ＬＡＮ９に接続されたアドレス発行サーバ１０は、ＬＡＮ９のアドレス情報またはＬＡＮ９に接続された通信機器１２、１３のアドレス情報を含む正規アドレス情報を中継装置６に向けて送信する。なお、このアドレス発行サーバ１０は、正規アドレス情報を定期的に送信するようにしてもよく、アドレス発行サーバ１０のオペレータによる起動に応じて送信するようにしてもよい。また、正規アドレス情報を送信するものとしては、アドレス発行サーバ１０の他にエッジルータ１１等のＬＡＮ９を構成する装置であれば何れのものでもよい。

【００７３】
図６において、正規アドレス情報格納部３８はさらに、アドレス発行サーバ１０によって送信された正規アドレス情報を正規アドレス情報格納部３８に追加するようになっている。
【００７４】
以上のように構成された分散型サービス不能攻撃防御システム１について、図７～図１０を用いてその動作を説明する。図７は、図１に示したゲート装置８の攻撃検知動作を示すフローチャートである。
【００７５】
まず、攻撃検知条件に基づいてネットワークインタフェイス２８によって受信されたパケットによる攻撃が攻撃検知部２０によって検知されると（ステップＳ１）、攻撃が検知されたパケットの特徴を表す容疑シグネチャが容疑シグネチャ生成部２１によって生成される（ステップＳ２）。
【００７６】
次に、容疑シグネチャに当てはまるパケットのうち、正規条件情報に表された条件に合うパケットの特徴を表す正規シグネチャが正規シグネチャ生成部２４によって生成されるとともに（ステップＳ３）、容疑シグネチャに当てはまるパケットのうち、不正条件に合うパケットの特徴を表す不正シグネチャが不正シグネチャ生成部２５によって生成される（ステップＳ４）。
【００７７】
次に、容疑シグネチャ、正規シグネチャおよび不正シグネチャがパケット制限部２６によるパケット通過条件として設定される（ステップＳ５）。また、容疑シグネチャおよび正規シグネチャがシグネチャ転送部２７によって隣接関係にある中継装置３および中継装置６に転送される（ステップＳ６）。
【００７８】
図８は、図１に示した中継装置６のシグネチャ受信動作を示すフローチャートである。まず、入力ポート３０に容疑シグネチャおよび正規シグネチャが受信されると（ステップＳ１０）、受信された容疑シグネチャに当てはまるパケットのうち、不正条件に合うパケットの特徴を表す不正シグネチャが不正シグネチャ生成部３５によって生成される（ステップＳ１１）。
【００７９】
次に、容疑シグネチャ、正規シグネチャおよび不正シグネチャがパケット制限部３６によるパケット通過条件として設定される（ステップＳ１２）。また、容疑シグネチャおよび正規シグネチャがシグネチャ転送部３７によって隣接関係にある中継装置５に転送される（ステップＳ１３）。さらに正規アドレス情報格納部３８に保持している正規アドレス情報を容疑シグネチャの送信元であるゲート装置８に送信する（ステップＳ１４）。
【００８０】
図９は、図１に示したゲート装置８のパケット制限動作を示すフローチャートである。まず、ネットワークインタフェイス２８にパケットが受信されると（ステップＳ２０）、受信されたパケットが不正シグネチャに当てはまるか否かがパケット制限部２６によって判断される（ステップＳ２１）。
【００８１】
パケットが不正シグネチャに当てはまると判断された場合には、パケットがパケット制限部２６によって廃棄される（ステップＳ２２）、一方、パケットが不正シグネチャに当てはまらないと判断された場合には、パケットが正規シグネチャに当てはまるか否かがパケット制限部２６によって判断される（ステップＳ２３）。
【００８２】
パケットが正規シグネチャに当てはまると判断された場合には、パケットの通過がパケット制限部２６によって許可される（ステップＳ２４）。一方、パケットが正規シグネチャに当てはまらないと判断された場合には、パケットが容疑シグネチャに当てはまるか否

かがパケット制限部２６によって判断される（ステップＳ２５）。

【００８３】

パケットが容疑シグネチャに当てはまると判断された場合には、容疑シグネチャに示された処理等に基づいて伝送帯域が絞られた経路を介したパケットの通過が許可される（ステップＳ２６）。一方、パケットが容疑シグネチャに当てはまらないと判断された場合には、パケットの通過がパケット制限部２６によって許可される（ステップＳ２４）。なお、中継装置３～６のパケット制限動作は、ゲート装置８のパケット制限動作と同様であるため説明を省略する。

【００８４】

図１０は、分散型サービス不能攻撃防御システム１の正規条件情報更新動作を示すシーケンス図である。まず、ＬＡＮ９のアドレス発行サーバ１０からＬＡＮ９内の正規アドレス情報が中継装置６に送信され（ステップＳ３０）、中継装置６の正規アドレス情報格納部３８に格納されるとともに（ステップＳ３１）、通信装置１６からの正規アドレス情報が中継装置５に送信され（ステップＳ３２）、中継装置５の正規アドレス情報格納部３８に格納される（ステップＳ３３）。

【００８５】

ここでゲート装置８において攻撃を検知すると（ステップＳ３４）、対応する容疑シグネチャが生成され（ステップＳ３５）、隣接する中継装置３および中継装置６に転送される（ステップＳ３６）。以下では、簡単のため中継装置３および中継装置４へのシグネチャの転送については記述を省略する。

【００８６】

中継装置６はゲート装置８から容疑シグネチャを受信すると、正規アドレス情報格納部３８に格納してある正規アドレス情報をゲート装置８に送り返し（ステップＳ３７）、容疑シグネチャをさらに中継装置５に転送する（ステップＳ４１）。ここで、ステップＳ３７とステップＳ４１は順序を逆にすることが可能である。

【００８７】

正規アドレス情報がゲート装置８のネットワークインタフェイス２８に受信されると、受信された正規アドレス情報に基づいて正規条件情報が正規条件情報生成部２３によって生成され、生成された正規条件情報を以って正規条件情報格納部２２に格納された正規条件情報が更新される（ステップＳ３８）。次いで、正規シグネチャ生成部２４にて、対応する正規シグネチャが生成され、パケット制限と中継装置６への転送が行なわれる（ステップＳ３９～Ｓ４０）。

【００８８】

一方、中継装置５は、中継装置６から容疑シグネチャを受信すると、正規アドレス情報格納部３８に格納してある正規アドレス情報を容疑シグネチャの送信元である中継装置、すなわち中継装置６に送信する（ステップＳ４２）。中継装置６は、中継装置５から受信した正規アドレス情報をそのままゲート装置８に送信する（ステップＳ４３）。

【００８９】

正規アドレス情報がゲート装置８のネットワークインタフェイス２８に受信されると、受信された正規アドレス情報に基づいて正規条件情報が正規条件情報生成部２３によって生成され、生成された正規条件情報を以って正規条件情報格納部２２に格納された正規条件情報が更新される（ステップＳ４４）。次いで、正規シグネチャ生成部２４にて、対応する正規シグネチャが生成され、パケット制限と中継装置６への転送が行なわれる（ステップＳ４５～Ｓ４６）。

【００９０】

以上説明したように、分散型サービス不能攻撃防御システム１によれば、ネットワーク２を介した攻撃を行わないパケットの送信元を表す正規アドレス情報がゲート装置８に送信され、ゲート装置８に送信された正規アドレス情報に基づいて、通信機器７に対する攻撃とみなされないパケットの条件を表す正規条件情報を更新するため、正規条件情報を容易に管理することができる。

【００９１】

なお、上記実施例に示したゲート装置８は、コンピュータにプログラムをロードして実行することにより機能発揮する。具体的には、コンピュータのＲＯＭ（Read Only Memory）等に容疑シグネチャを送信して正規アドレス情報を取得するルーチン、正規アドレス情報に基づいて非攻撃パケットの条件を示す正規条件情報を生成するルーチン、ネットワークから受信したパケットのうち正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器へ攻撃をおこなうパケットの通過を制限するルーチンを含むプログラムを記憶しておき、かかるプログラムをＣＰＵにロードして実行することにより、本発明に係るゲート装置８を形成することができる。

【産業上の利用可能性】

【００９２】

以上のように、本発明にかかるサービス不能攻撃防御システム、サービス不能攻撃防御方法およびサービス不能攻撃防御プログラムは、サービス不能攻撃および分散型サービス不能攻撃から通信機器を防御する場合に適している。

【図面の簡単な説明】

【００９３】

【図１】本実施例に係る分散型サービス不能攻撃防御システムの構成を示すブロック図である。

【図２】図１に示したゲート装置の構成を示すブロック図である。

【図３】本実施例に係る攻撃検知条件の一例を示す図である。

【図４】本実施例に係る正規条件情報の一例を示す図である。

【図５】本実施例に係る不正条件の一例を示す図である。

【図６】図１に示した中継装置の構成を示すブロック図である。

【図７】図２に示したゲート装置の攻撃検知動作を示すフローチャートである。

【図８】図６に示した中継装置のシグネチャ受信動作を示すフローチャートである。

【図９】図２に示したゲート装置のパケット制限動作を示すフローチャートである。

【図１０】本実施例に係る分散型サービス不能攻撃防御システムの正規条件情報更新動作を示すシーケンス図である。

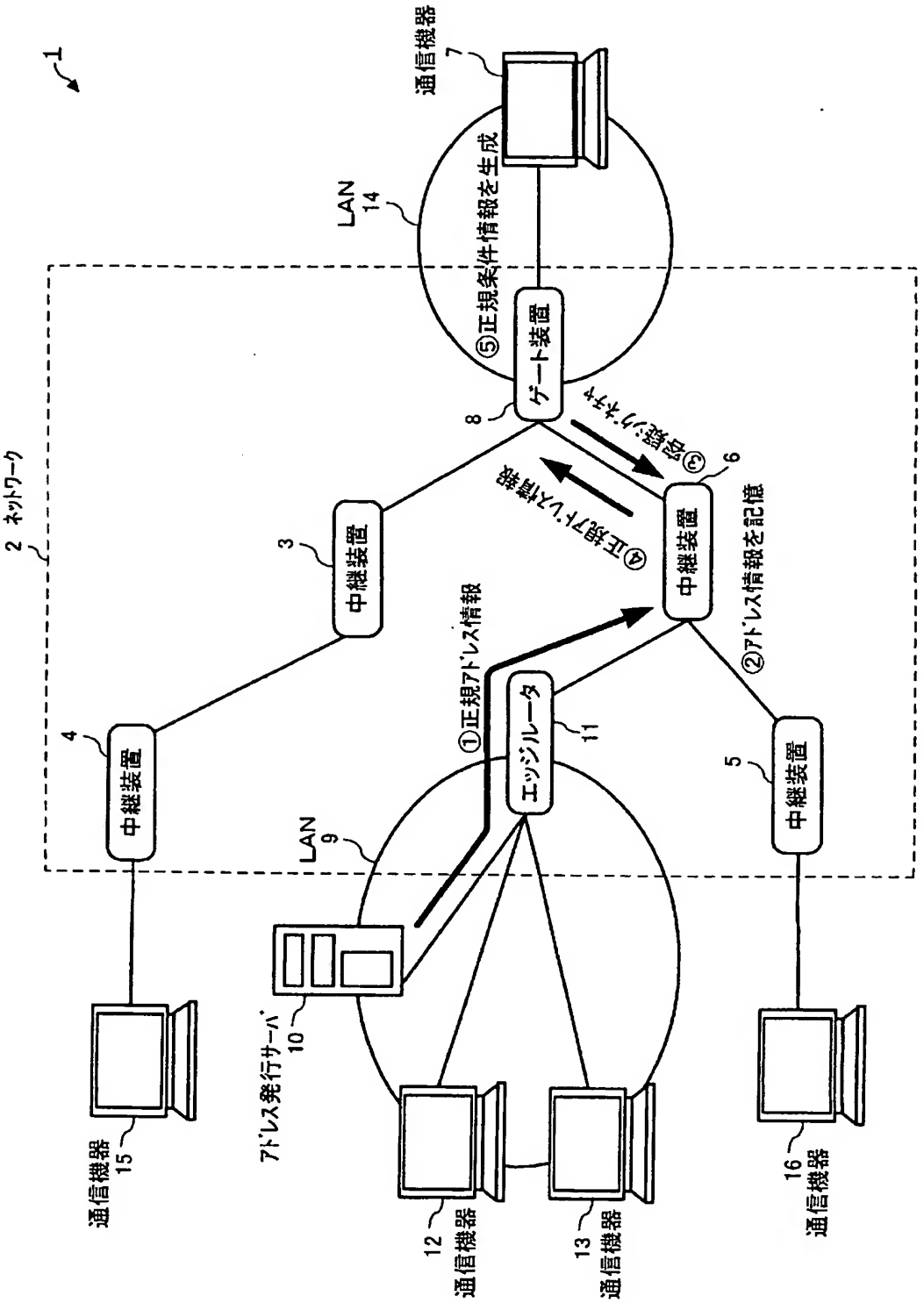
【符号の説明】

【００９４】

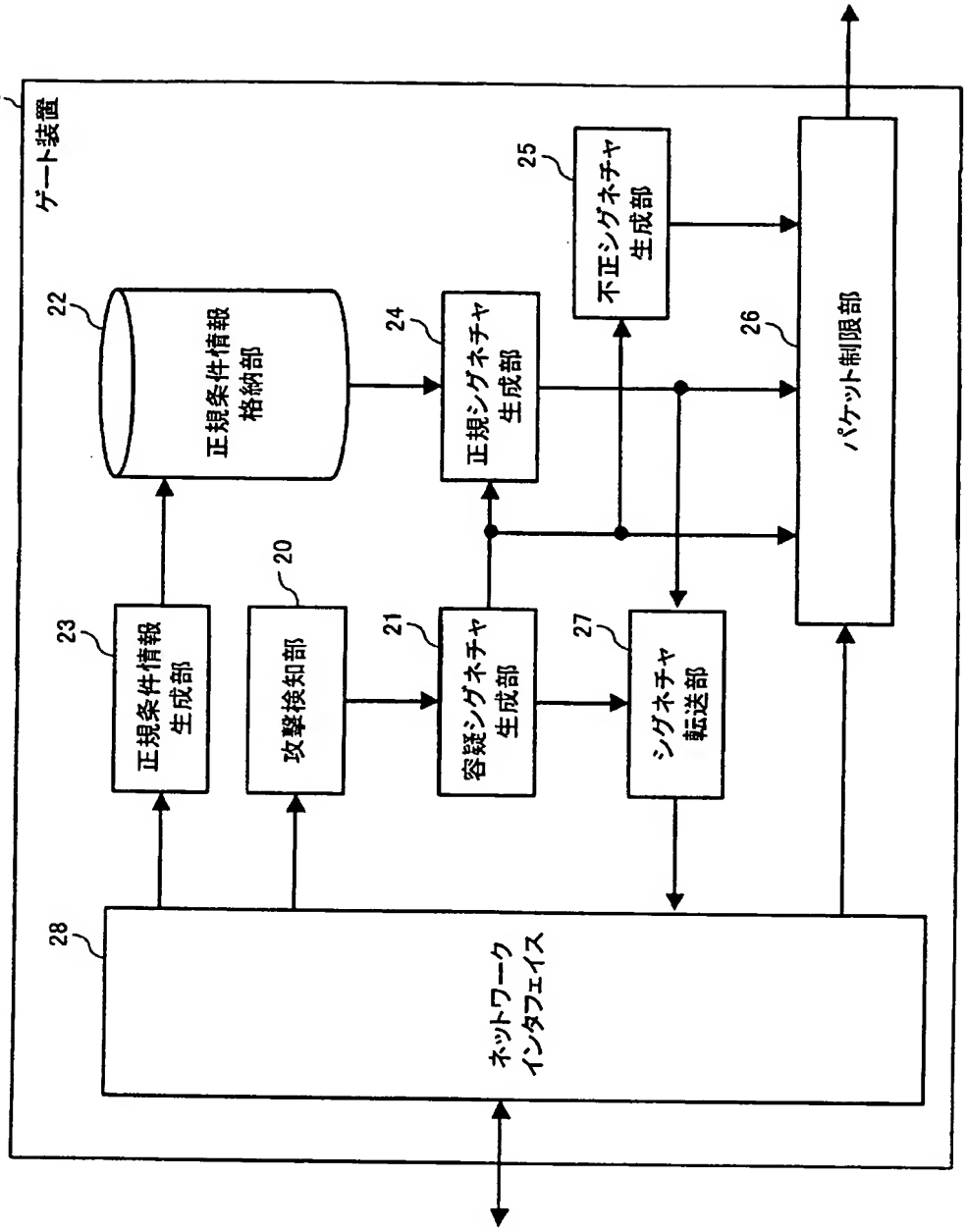
１　分散型サービス不能攻撃防御システム
２　ネットワーク
３、４、５、６　中継装置
７　通信機器
８　ゲート装置
９　ＬＡＮ
１０　アドレス発行サーバ
１１　エッジルータ
１２、１３、１５、１６　通信機器
１４　ＬＡＮ
２０　攻撃検知部
２１　容疑シグネチャ生成部
２２　正規条件情報格納部
２３　正規条件情報生成部
２４　正規シグネチャ生成部
２５、３５　不正シグネチャ生成部
２６、３６　パケット制限部
２７、３７　シグネチャ転送部
２８　ネットワークインタフェイス
３０　入力ポート

３１　スイッチ
３２　出力ポート
３８　アドレス情報記憶部
３９　正規アドレス情報送信部

【書類名】図面
【図１】


1
2 ネットワーク
3 中継装置
4 中継装置
5 中継装置
6 中継装置
7 通信機器
8 ゲート装置
9 LAN
10 アドレス発行サーバ
11 エッジルータ
12 通信機器
13 通信機器
14 LAN
15 通信機器
16 通信機器
①正規アドレス情報
②アドレス情報を記憶
③登録リクエスト
④正規アドレス情報
⑤正規案件情報を生成

【図２】


8
ゲート装置
22
正規条件情報
格納部
24
正規シグネチャ
生成部
25
不正シグネチャ
生成部
26
パケット制限部
23
正規条件情報
生成部
20
攻撃検知部
21
容疑シグネチャ
生成部
27
シグネチャ
転送部
28
ネットワーク
インタフェイス

【図３】

	検知属性	検知閾値	検出時間
1	{Dst=192.168.1.1/32, Protocol=TCP, Port=80}	500kbps	10秒
2	{Dst=192.168.1.2/32, Protocol=UDP}	300kbps	10秒
3	{Dst=192.168.1.0/24}	1Mbps	20秒

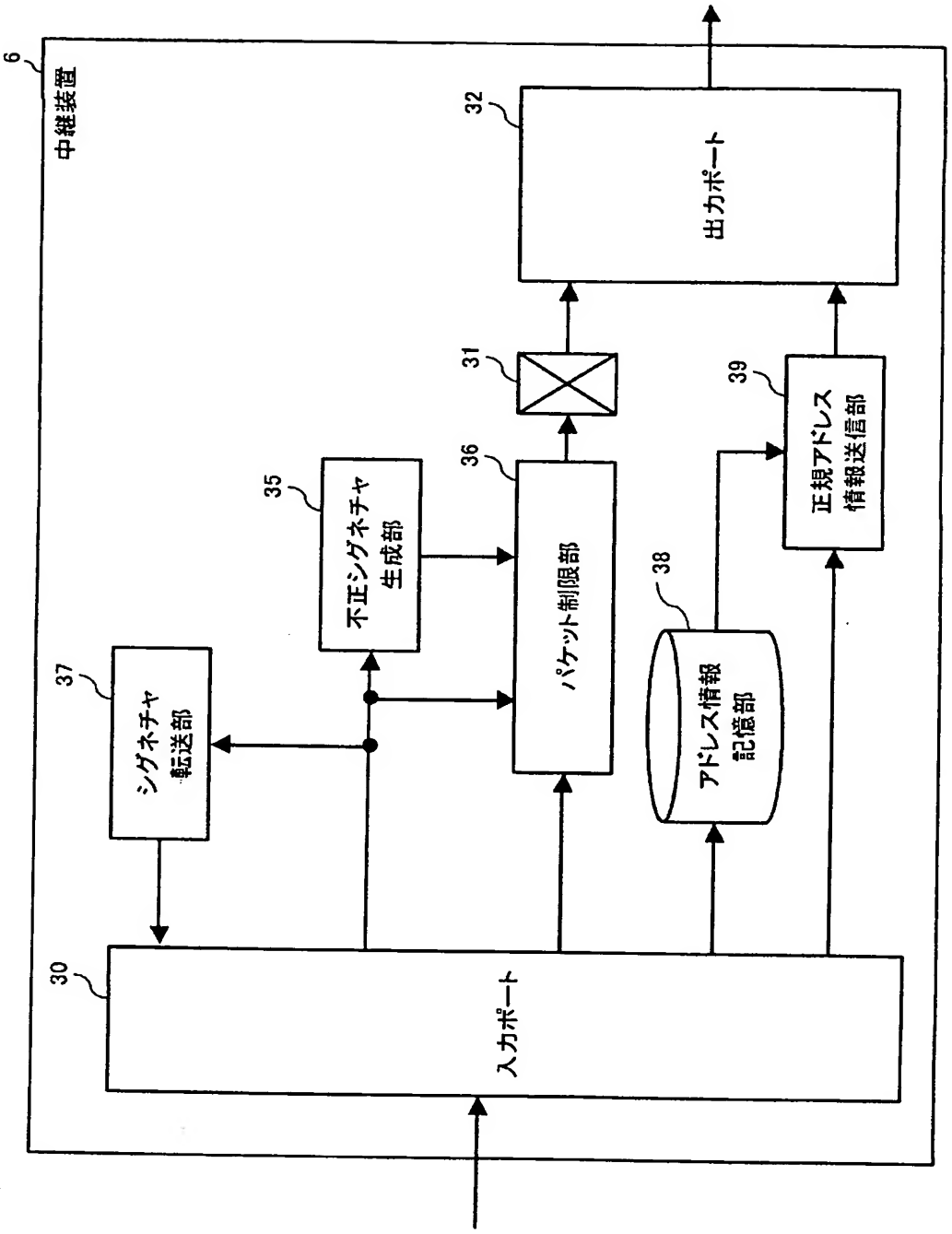
【図４】

	正規条件
1	{Src=172.16.10.0/24}
2	{TOS=0x01}

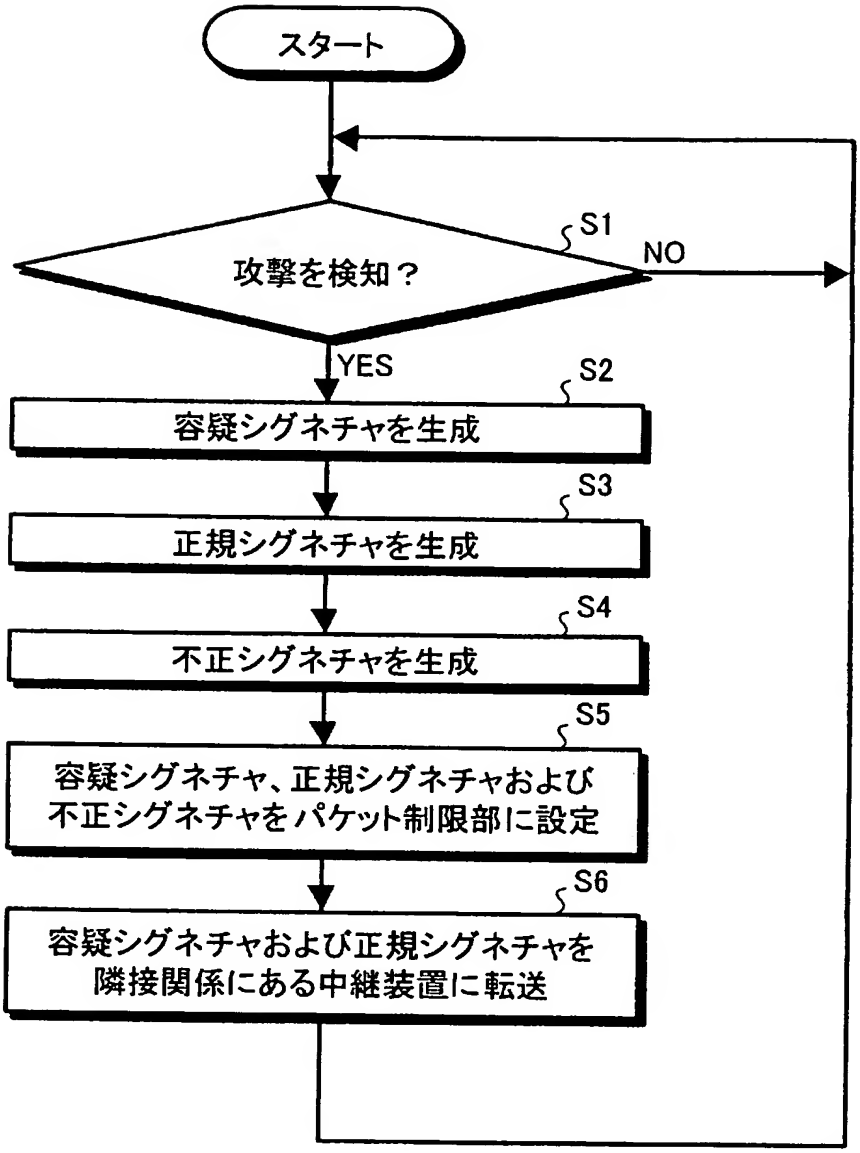
【図５】

	不正条件
1	500kbps以上のパケットが30秒以上連続送信されている
2	300kbps以上のICMP/Echo Replyパケットが15秒以上連続送信されている
3	300kbps以上のフラグメントパケットが15秒以上連続送信されている

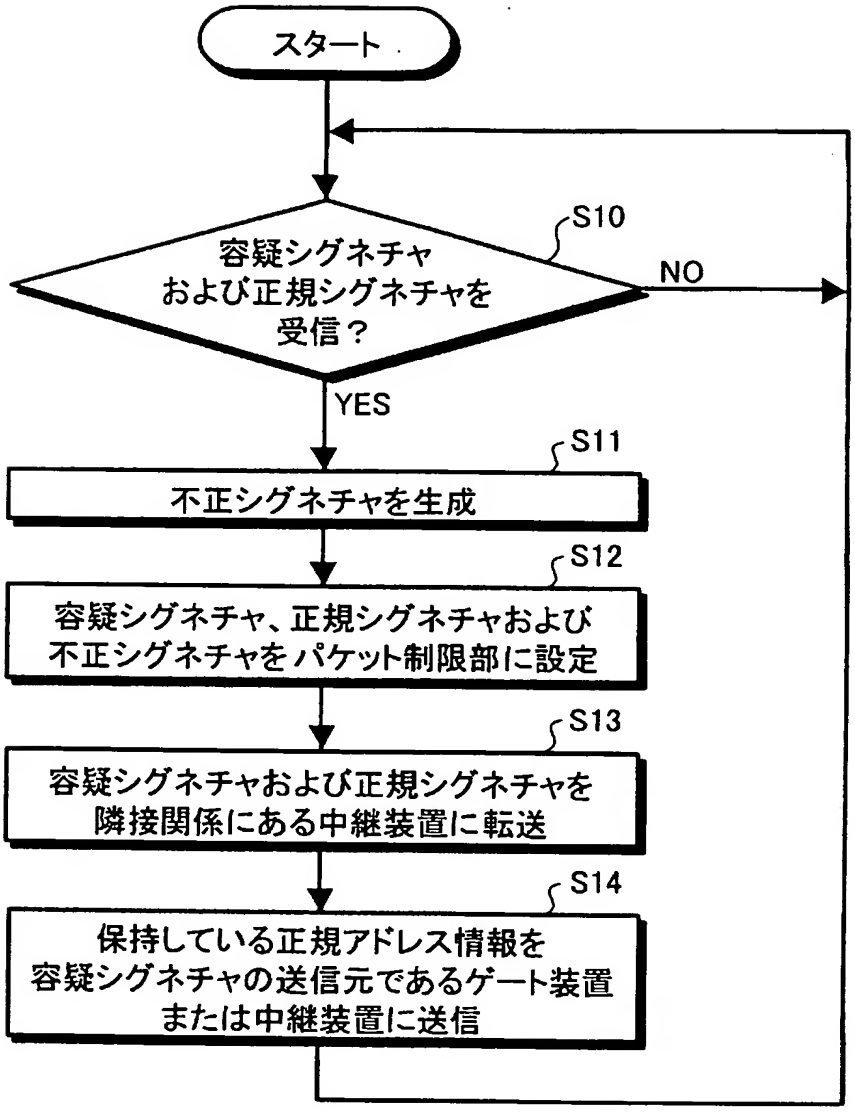
【図６】


6
中継装置
32
出力ポート
31
39
正規アドレス
情報送信部
35
不正シグネチャ
生成部
36
パケット制限部
38
アドレス情報
記憶部
37
シグネチャ
転送部
30
入力ポート

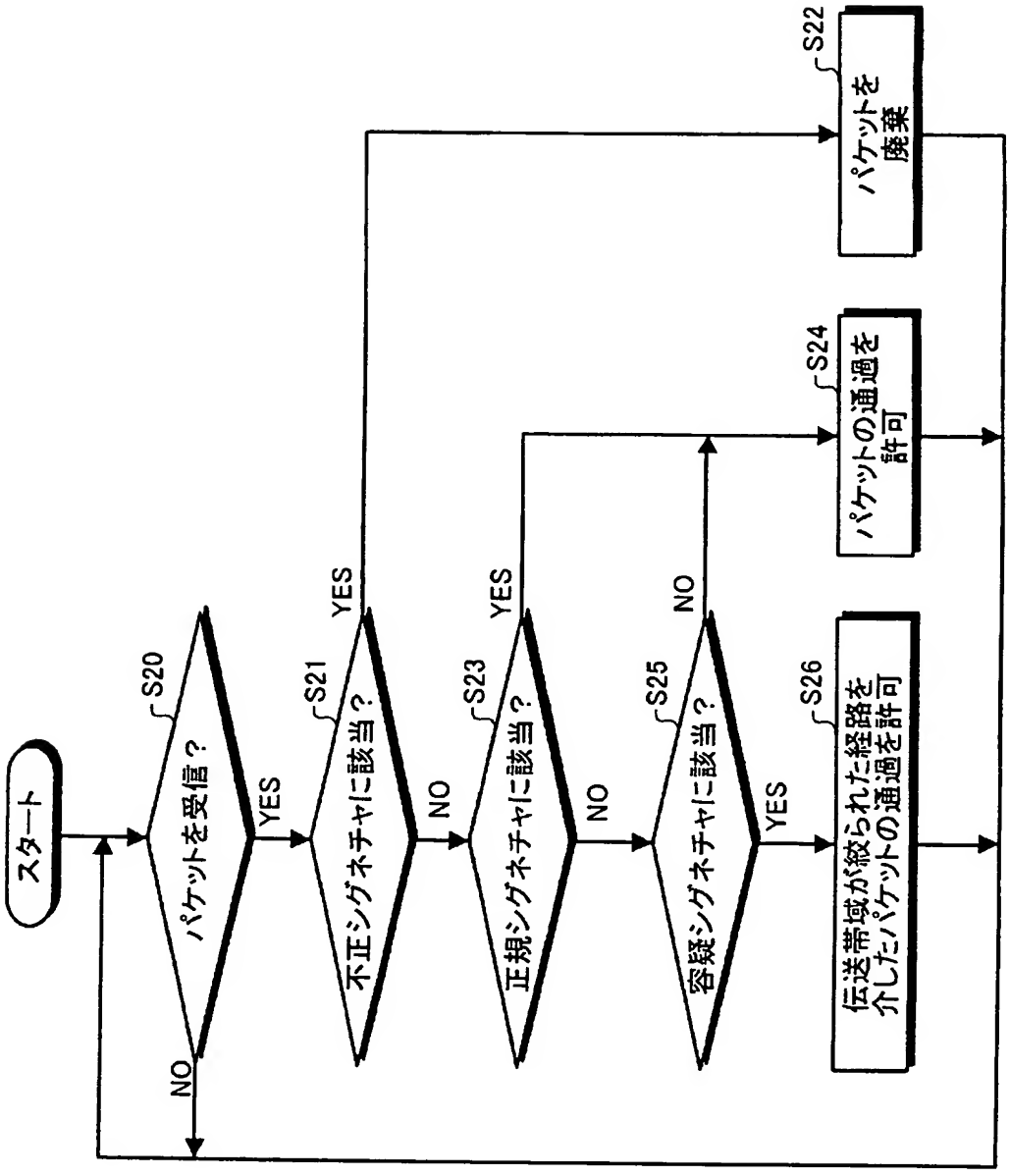
【図７】


スタート
S1
攻撃を検知？
NO
YES
S2
容疑シグネチャを生成
S3
正規シグネチャを生成
S4
不正シグネチャを生成
S5
容疑シグネチャ、正規シグネチャおよび
不正シグネチャをパケット制限部に設定
S6
容疑シグネチャおよび正規シグネチャを
隣接関係にある中継装置に転送

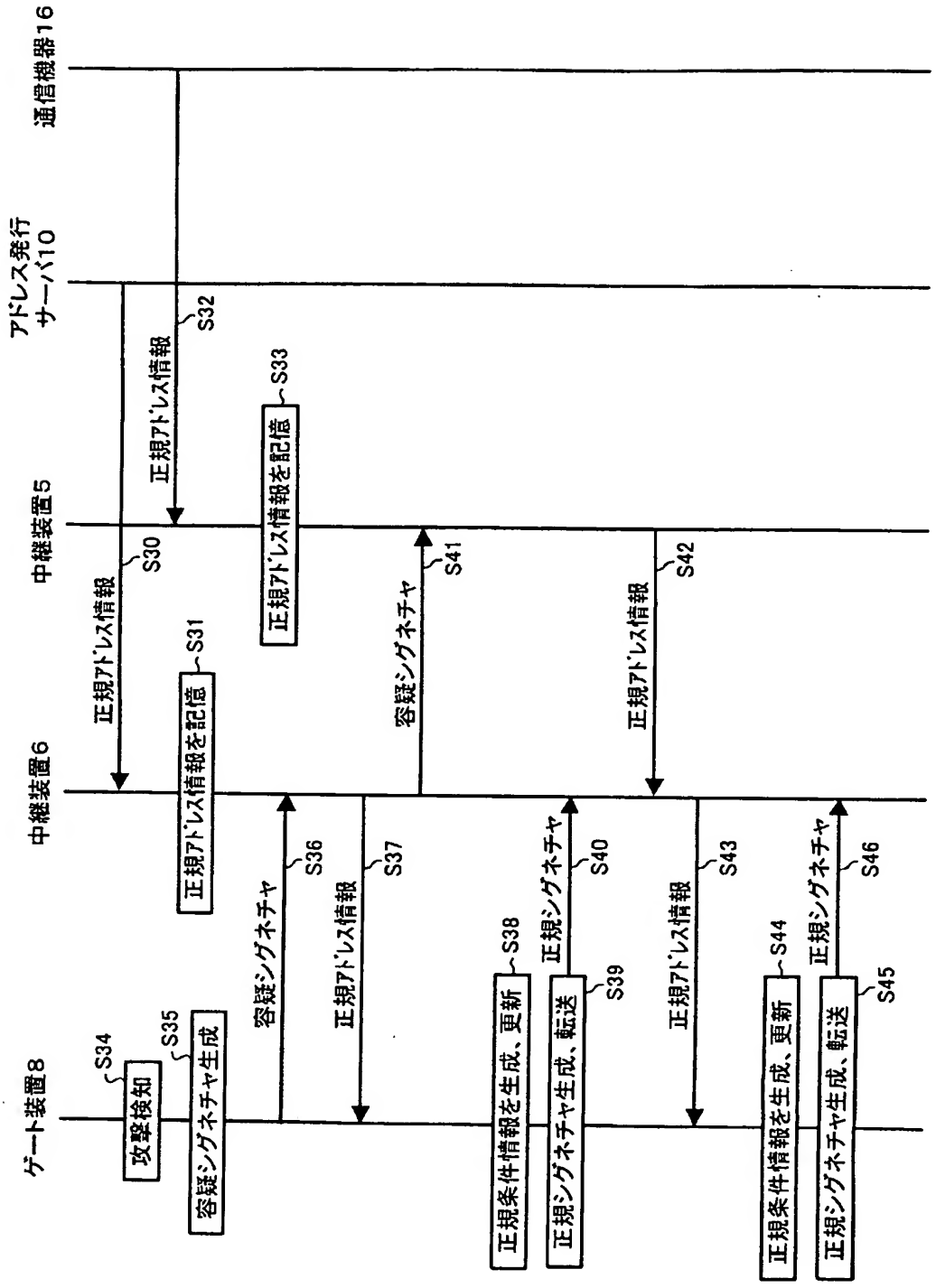
【図８】


スタート
S10
容疑シグネチャ
および正規シグネチャを
受信？
NO
YES
S11
不正シグネチャを生成
S12
容疑シグネチャ、正規シグネチャおよび
不正シグネチャをパケット制限部に設定
S13
容疑シグネチャおよび正規シグネチャを
隣接関係にある中継装置に転送
S14
保持している正規アドレス情報を
容疑シグネチャの送信元であるゲート装置
または中継装置に送信

【図９】


スタート
S20
パケットを受信？
YES
NO
S21
不正シグネチャに該当？
YES
NO
S22
パケットを廃棄
S23
正規シグネチャに該当？
YES
NO
S24
パケットの通過を許可
S25
容疑シグネチャに該当？
NO
YES
S26
伝送帯域が絞られた経路を介したパケットの通過を許可

【図１０】


ゲート装置8
中継装置6
中継装置5
アドレス発行サーバ10
通信機器16
正規アドレス情報
S30
正規アドレス情報
S32
正規アドレス情報を記憶
S33
正規アドレス情報を記憶
S31
容疑シグネチャ
S41
正規アドレス情報
S42
攻撃検知
S34
容疑シグネチャ生成
S35
容疑シグネチャ
S36
正規アドレス情報
S37
正規条件情報を生成、更新
S38
正規シグネチャ
S40
正規シグネチャ生成、転送
S39
正規アドレス情報
S43
正規条件情報を生成、更新
S44
正規シグネチャ
S46
正規シグネチャ生成、転送
S45

【書類名】要約書
【要約】
【課題】防御対象の通信機器に対して攻撃をおこなわない非攻撃パケットの条件を表す正規条件情報を容易に管理することを課題とする。
【解決手段】ネットワーク２上に所在する正当な装置（アドレス発行サーバ１０）により送信された非攻撃パケットの送信元を示す正規アドレス情報をゲート装置８が取得し、取得した正規アドレス情報に基づいてゲート装置８が非攻撃パケットの条件を示す正規条件情報を生成し、ネットワークから受信したパケットのうち正規条件情報に示された条件に適合するパケットの通過を許容しつつ、通信機器７へ攻撃をおこなうパケットの通過を制限する。
【選択図】　図１

出願人履歴

０００００４２２６
19990715
住所変更
５９１０２９２８６

東京都千代田区大手町二丁目３番１号
日本電信電話株式会社

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record.

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☑ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.